(i) Repeater: The function of repeater is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network.

(ii) Hub: A hub connects multiple users coming from different branches, eg. the connector in star topology which connects different stations. Hubs cannot filter data, so data packets all sent to all connected devices.

(iii) Bridge: A bridge operates at the data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC address of source and destination. It is also used for interconnecting 2 LAN's working on same protocol.

(iv) Switch: Switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.

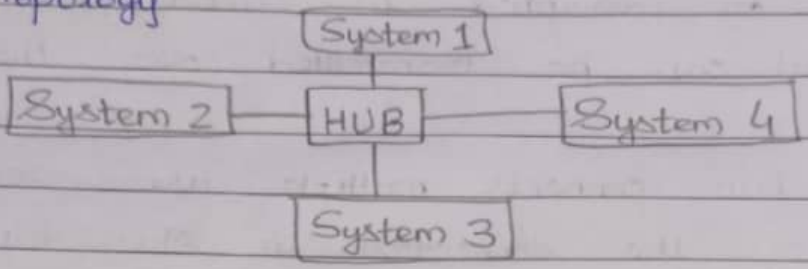
23/01/24

(v) Router: Router plays a critical role in directing data traffic between different networks and facilitate communication devices on separate IP subnets.

(vi) Gateways : A gateway serves as a point of entry or exit between 2 different networks that use different communication protocols.

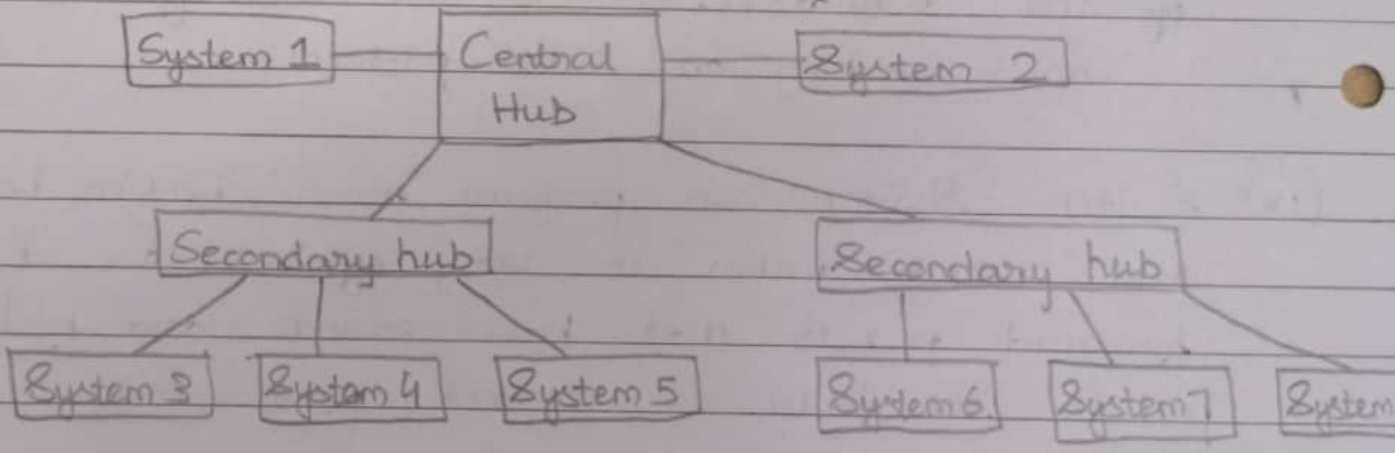
* Comparing all topologies

① Star Topology



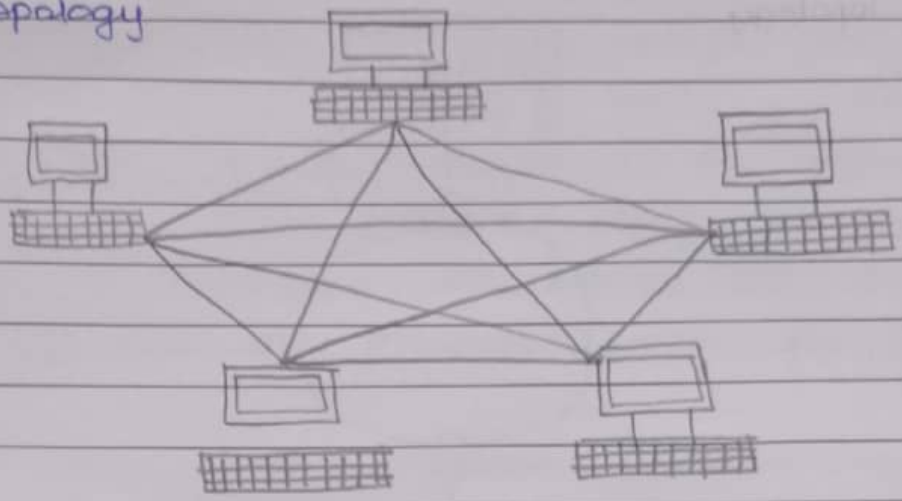
- All devices connected to a central hub / switch.
- Easy to install and manage.
- Failure of one cable or device does not affect others.
- Requires more cabling than bus topology.

② Tree Topology



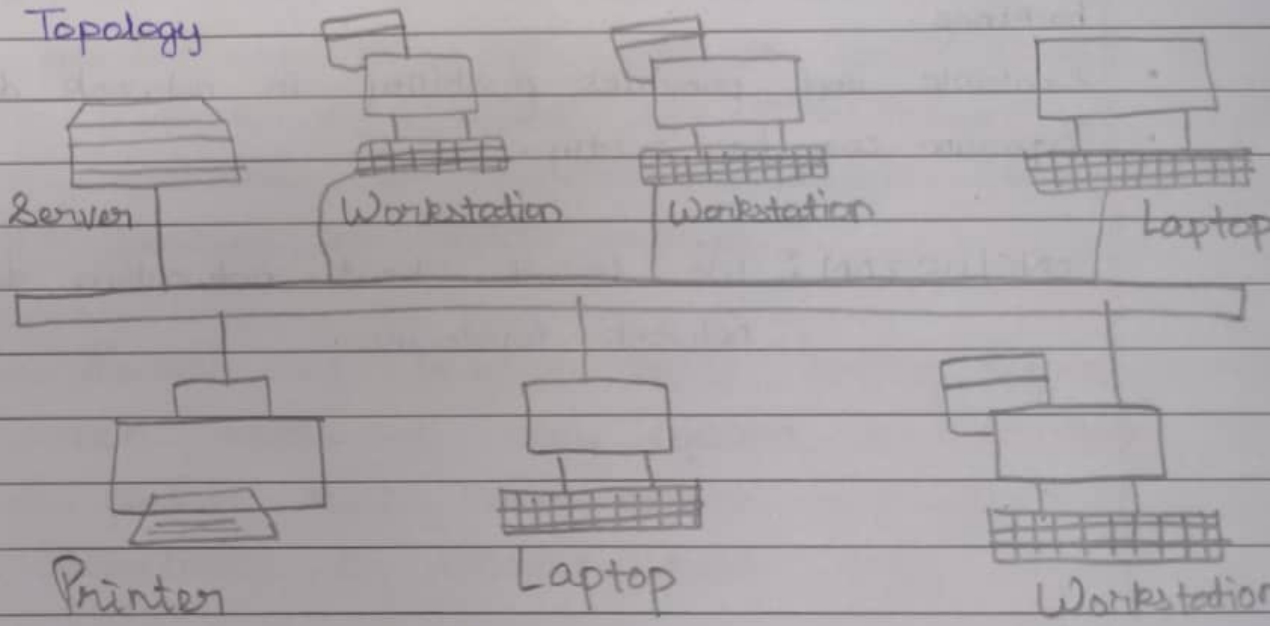
- Devices connected in a circular fashion.
- Data travels in one direction, simplifying data collision is
- If one device or connection fails, the center network may be disrupted.

③ Mesh Topology



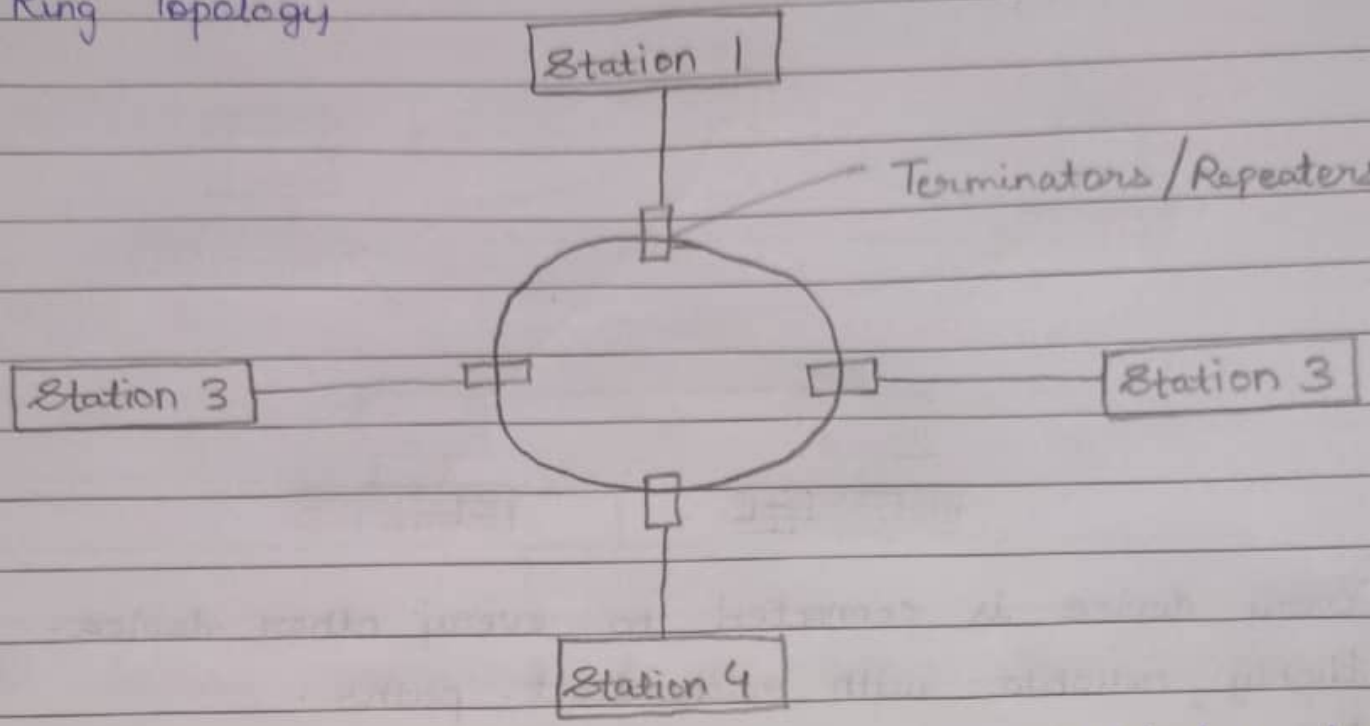
- Every device is connected to every other device.
- Highly reliable with redundant paths.
- Data can take multiple routes, improving tolerance.

④ Bus Topology



- Single central cable (bus) connecting all devices
- Simple and cost effective per small networks.
- Easy to set up and expand.
- Suspectible to a single point of failure (central cable).

⑤ Ring Topology



- Topology combining characteristics of star and bus topologies.
- Groups of star configured networks connected to a bus backbone.
- Scalable and provides flexibility in network design.
- Expansion can be costly.

CONCLUSION: We learnt about networking devices and network topologies.

Q. An ISP is granted a block of addresses starting with 190.100.0.0. The ISP needs to distribute these addresses to 3 groups of customers as follows:

(a) The first group has 64 customers; each need 256 addresses
(b) The 2nd group has 128 customers; each need 128 addresses
(c) The 3rd group has 128 customers; each needs 64 addresses.

Design the sublocks and find out how many addresses are still available after these allocations.

(a) Group 1 requires 256 addresses = 2^8 bits

∴ Prefix length = 32 − 8 = 24.

	First add	Last add
1st Customer	192.100.0.0/24	192.100.0.256/24
2nd Customer	192.100.1.0/24	192.100.1.256/24
64th Customer	192.100.63.0/24	192.100.63.256/24

(b) Group 2 requires 128 addresses = 2^7 bits.

∴ Prefix length = 32 − 7 = 25.

	First add	Last add
1st Customer	192.100.64.0/25	192.100.64.127/25
2nd Customer	192.100.64.128/25	192.100.64.256/25
128th Customer	192.100.127.128/25	192.100.127.256/25

(c) Group 3 requires 64 addresses = 2^6 bits

∴ Prefix length = 32 − 6 = 26.

	First add	Last add
1st Customer	192.100.128.0/026	192.100.127.63/26
2nd Customer	192.100.128.64/26	192.100.159.256/26
128th Customer	192.100.159.192/26	192.100.127.256/26

Q. Complete the subnet mask for class C for host 30 and write down the steps.

Soln: Determine the no. of host bits required to accomodate 30 hosts.

$\log_2 32 = 5$.

∴ To find remaining subnet bits

= 32 − 5

= 27

∴ The first 27 bits would be all followed by 5 bits of 0's

So the subnet mask would be

(11111111.11111111.11111111.11100000)

∴ The subnet mask for a class C network accomodating 30 hosts is

(255.255.255.224).

OSI Model – 7 layer architecture

- Application Layer – Provides services for network applications with help of protocols to perform user activities.
  Eg: HTTPS, SMTP, FTP, Telnet – Protocols used in Application Layer.

- Presentation Layer – Receives data from application layer. This data is in form of characters and numbers. Presentation layer converts this to machine understandable format, that is binary. Presentation layer performs data compression, data encryption. SSL (Secured Socket Layer) protocol is used for data encryption.

- Session Layer – Helps in establishing and terminating the connections. Session layer uses APIs for this case. Before a connection is established, there is a process 'Authentication' done by server. After this, authorization is checked. Images and text downloaded from internet are in the form of packets and session layer keeps tracks of these packets separately.

- Transport Layer – Controls reliability of communication through segmentation, flow control, error control.
  Segmentation – Data received from session layer is divided into smaller units 'segments'. Each segment contains source, destination port number and a sequance number. This guides segments to correct apps. Sequance no. helps to redirect segments in correct order.

- Network Layer - Works for transmission of received data from one computer to another located in different networks. Layer where routers recide. N.L. assigns IP address to sender and receiver to each segment to form an IP packet.

- Data Link Layer - Receives data from Network Layer in form of Data Packets. Data Packet contains IP addressing of sender and receiver. There are 2 types of addressing Logical and Physical. Logical addressing is done at network layer where IP address is assigned. Physical addressing is done at DLL where MAC address of each data packet is assigned to sender and receiver. MAC address is a 12 digit alphanumeric number embedded in network interface card of computer by computer manufacturer. Data unit in DLL is called Frame.

- Physical Layer - Converts the data received in binary form to signals. The signals vary according to the type of media used.

* TCP/IP - Set of protocols that support network communication.

Application	HTTP	FTP	DNS	POP 3
Transport	TCP	UDP		
Network	IP	ICMP	IGMP	ARP
Data Link	Ethernet			
Physical	Ethernet			

- Physical — Layer where actual communication takes place. Binary format is converted to signals - and transmits them to local media. Local media is copper cable/LAN cable, Optical fiber, air or vacuum. Most common protocol used at physical layer is Ethernet.

- Data Link Layer — Data unit at DLL is called Ethernet frame. DLL is divided in 2 parts: Medium Access Control (MAC) sub layer and Logical Link Control (LLC) sub layer. MAC sub layer is responsible for Data encapsulation and accessing the media. For accessing the media, CSMA is used.

- Network Layer — Transfer TCP segments or UDP datagram to network layer. Network Layer then adds IP address to these TCP segments to form IP packets and then uses routers to send IP packets to the network. Logical Addressing, Routing and Path determination are tasks performed by Network Layer.

- Transport Layer — TL receives data from NL. When message is received in transport layer, then one of the two protocols i.e. TCP or UDP is selected. TCP, UDP full process.

- Application Layer — Used by user apps that pass messages from one computer to another in a network. All protocols in Application Layer - Explain.

* Data - Link Layer :

- Hop to Hope Delivery
  Node to Node

- Flow Control : DLL responsibility is to synchronize Sender's and receiver's speeds and establish flow control b/w them. DLL ka flow control works on flow control at every node whereas Transport layer ka flow control works like from source node to destination node.

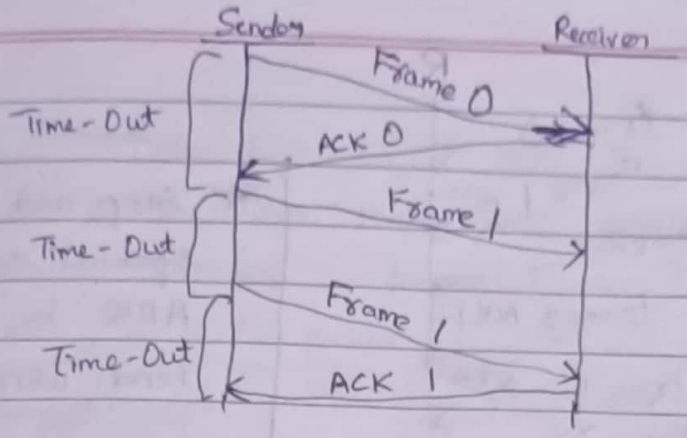
- Error Control : DLL's error control, controlls the error node to node. Three methods of error control which are used (Cyclic redundancy check, CheckSum, Parity).

- Access Control : When multiple devices share same communication channel, there is a high probability of collision, so it's the responsibility of DLL to check which device has control over the CSMA/CD and CSMA/CA can be used to avoid collisions and loss of frames in the channel.

* Stop and Wait ARQ : • It uses a link b/w sender and receiver as a half-duplex link.

- Throughput = 1 Data packet / frame per RTT.
- An eg. of "closed loop OR connection-oriented protocol".
- It is a special category of SWP where its window size is 1

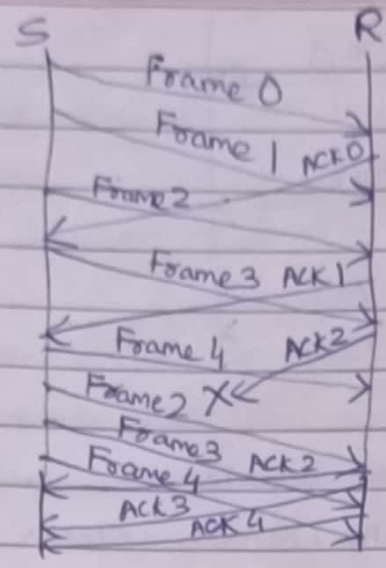
Adv : → Simple Implementation both in hardware, software.
→ Detects errors. → Reliable. → Flow Control.
Disadv : → Low efficiency. → High Latency. → Limited error recov



Sender maintains a timeout counter.
When a frame is sent, the sender starts the timeout counter.
If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
If acknowledgement doesn't come in time, the sender assumes that either the frames or its acknowledgement is lost in transit. Sender retransmits the frame & starts the timeout counter.
If a negative acknowledgement is received, the sender retransmits the frame.

Go-back-N ARQ

Stop-and-Wait ARQ mechanism doesn't utilize the resources at their best.
When the acknowledgement is received, the sender sits idle.
In Go-Back-N ARQ method, both sender and receiver maintain a window.
The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of previous one.
The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.
When the sender sends all frames in a window, it checks up to what sequence number it has received positive acknowledgement.
If all frames are positively acknowledged, sender sends next set of frame.
If sender finds that it has received NACK (negative acknowledgement) or has not received any ACK for a particular frame, it retransmits all frames after which it doesn't receive any ACK.

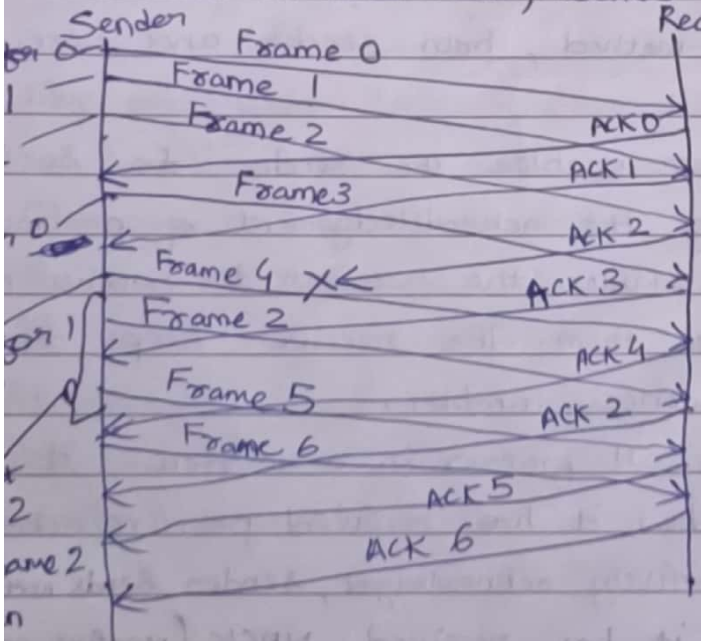


* Stop and wait ARQ is a special case of Go-back-N ARQ in which size of send window is 1.

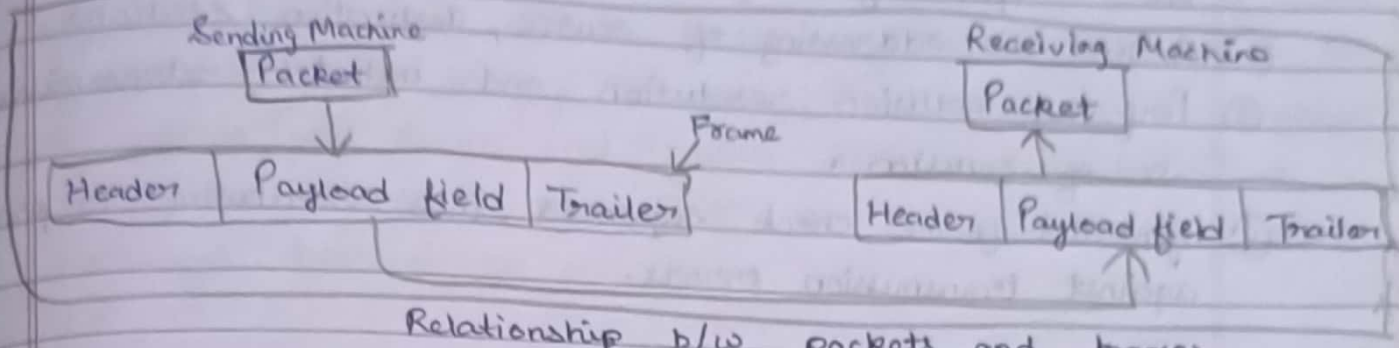
Selective Repeat

In Go-Back-N ARQ, it is assumed that receiver doesn't have any buffer space for its window size and has to process each frame as it comes.
This enforces the sender to retransmit all frames which are not acknowledged.

In selective-repeat-N ARQ, the receiver while keeping track of sequence numbers, buffers in memory and sends NACK for only one frame which is missing or damaged.
The sender in this case, sends only packet for which NACK is receive



* Framing : • Data link layer takes packets it gets from network layer and encapsulates them into frames for transmission.
• Each frame contains a frame header, a payload field for holding the packet, and a frame trailer.



Relationship b/w packets and frames.

* Hamming Code for Error detection and Correction
→ Formula for finding parity = 2^n → Jo bhi 2^n ke position pe aayega woo parity bit, baaki sab data bit.
For eg: 7 bit me
$2^n = 0, 1, 2 \Rightarrow n$
Positions → 1, 2, 4 parity bit honge 7 bit me baaki sab data bit.

Eg:

Positions	7	6	5	4	3	2	1
Bit	d_3	d_2	d_1	p_2	d_0	p_1	p_0
	1	0	1		0		

$p_2 = d_3 \oplus d_2 \oplus d_1$
$p_1 = d_3 \oplus d_2 \oplus d_0$
$p_0 = d_3 \oplus d_1 \oplus d_0$

$p_2 = 1 \oplus 0 \oplus 1 = 0$
$p_1 = 1 \oplus 0 \oplus 0 = 1$
$p_0 = 1 \oplus 1 \oplus 0 = 1$

* Cyclic Redundancy Check (CRC):
$x^4 + x^3 + 1 = 1x^4 + 1x^3 + 0x^2 + 0x^1 + 1$

x ke highest power ~~ho~~ 0 leke question me append karna hai.

Agar poly. na diya ho to division ke (bits − 1) kare append karna us me

Phir divisor ke liye Polynomial ka har power represent karke uska coefficient likhna hai.

```
          1 1 1 1
      ------------------
11001 | 1010 1010 0000
        11001
        -----
        11000
        11001
        -----
        11000
        11001
        -----
        11000
        11001
        -----
        00010
```

BW = Bandwidth

* Medium Access Control : 2 layers → Logical link control (LLC)
  → Medium Access Control (MAC)

Functions of MAC : ① Provides abstraction of physical layer to LLC & upper layer of OSI network.
② Resolve the addressing of source, destination stations.
③ Performs collision resolution and initiates retransmissions in case of collision.
④ Generates frame check sequences, thus contributing to protection against transmission errors.

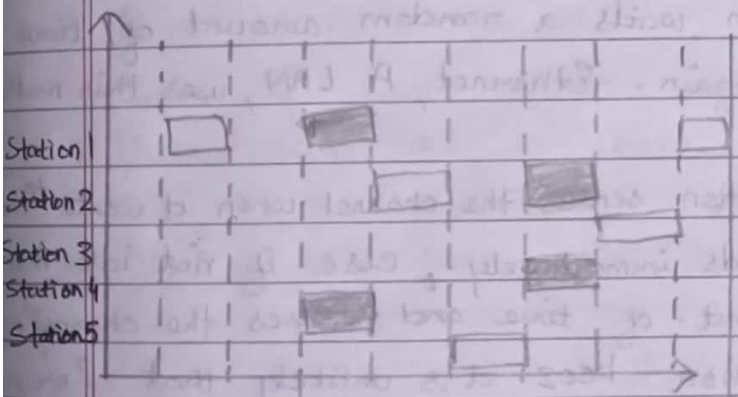
⇒ Channel Allocation Problem : ① When more than one user desires to access a shared network channel, an algo. is deployed for channel allocation among competing users.
② Network channel may be single cable or optical fiber connecting multiple nodes.
③ Channel allocation algo. allocates the wired channels & bandwidth to users.

- Static Channel Allocation : ① Fixed portion of frequency channel is allocated to each user.
② For N competing users, Bandwidth is divided into N channels using frequency division multiplexing (FDM), & each portion is assigned to one user
③ In this scheme, there is no interference b/w users since each user is assigned a fixed channel.

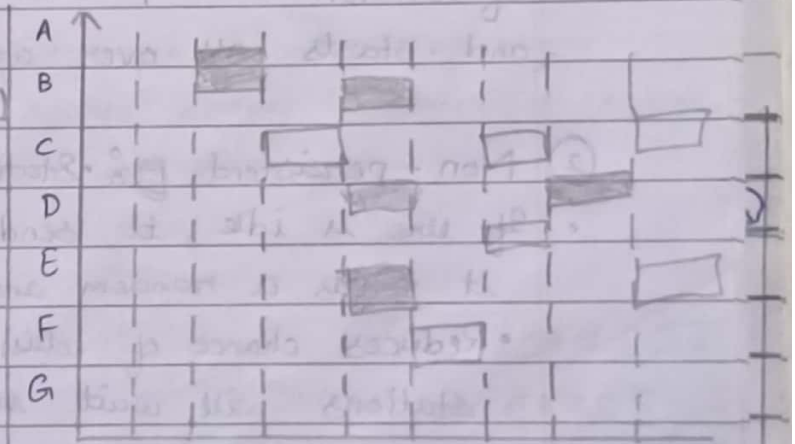
- Dynamic Channel Allocation : ① Frequency bands aren't permanently assigned to users. Instead, channels are allocated dynamically as needed, from a pool
② This allocation scheme optimises BW usage and results in faster transmission.

* ALOHA: - Is a multiple access protocol for transmission of data via shared network. Operates in medium access control sublayer. Each node or station transmits a frame without trying to detect whether transmission channel is busy or not. If channel is idle, then frames will be successfully transmitted else if two frames attempt to occupy the channel simultaneously, then collision of frames will occur and frames will be discarded. Those station may choose to retransmit the corrupted frames until successful transmission occurs.

Q.	Pure Aloha	Slotted Aloha
①	Any station can transmit data at any time	Any station can transmit data at beginning of any time slot.
②	Time is continuous, not globally synced.	Time is discrete, globally synced.
③	Vulnerable time in which collision may occur = $2 \times T$	Vulnerable time in which collision may occur is T.
④	Probability of successful transmission of data packet = $G \times e^{-2G}$	Probability of successful transmission of data packet = $G \times e^{-G}$
⑤	Max efficiency = 18.4%. Occurs at $G = 1/2$.	Max efficiency = 36.8%. Occurs at $G = 1$.
⑥	Adv: Easy to implement.	Adv: Reduces no. of collisions to half and doubles the efficiency of pure aloha



(Shaded slots indicate collisions).



Slotted Aloha Protocol (shaded slots indicate collision).

* Carrier Sense Multiple Access (CSMA)

- To minimize chance of collision and therefore increase performa
- Chance of collision can be reduced if a station senses the medium before trying to use it.
- CSMA requires that each station first listen to the medium before sending.
- CSMA is based on principle of "sense before transmit" or "listen before talk". It can reduce possibility of collisions, but it can't eliminate it.

⇒ If the channel is busy or idle then what action station has to take is ~~decided~~ identified by 3 persistent techniques.
① 1 persistent. ② Non persistent ③ P-persistent.

Vulnerable Time :— Time needed for a signal to propagate from one end of medium to another.
↓
Propagation Time (T_p)

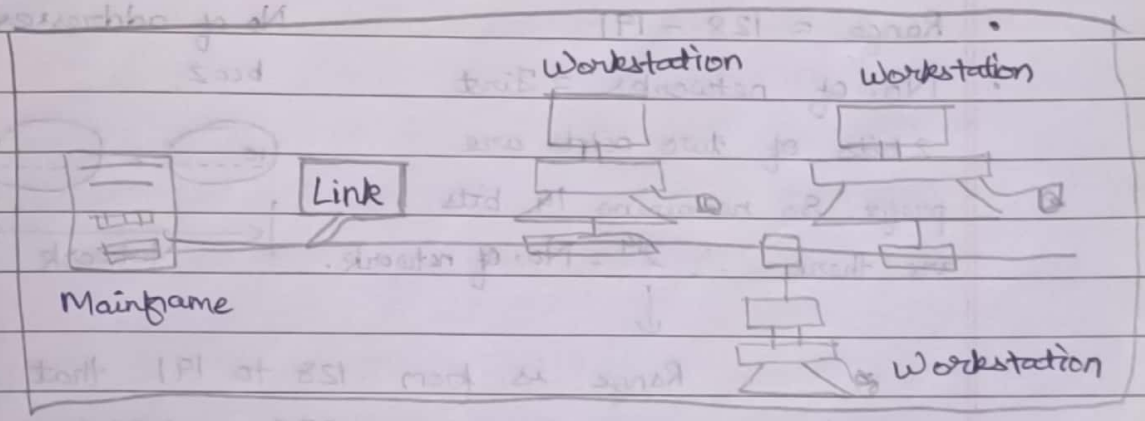
① 1 persistent : • When station needs to send data, it first listens to channel
- If channel is busy, station waits for it to become free.
- When channel becomes free, station can transmit a frame.
- Collision occurs when 2 station detect an ~~empty~~ idle channel simultaneously and send frames simultaneously.
- If collision occurs, station waits a random amount of time and starts all over again. Ethernet, A LAN, uses this method.

② Non-persistent : • Station senses the channel when it wants to send da
- If line is idle, it sends immediately, else if not idle then it waits a random amt. of time and senses the channel again
- Reduces chance of collision beoz it is unlikely that 2 or more stations will wait same amt. of time and retry to send immediately.
- Reduces efficiency of network beoz medium remains idle when there stations with frame to send.

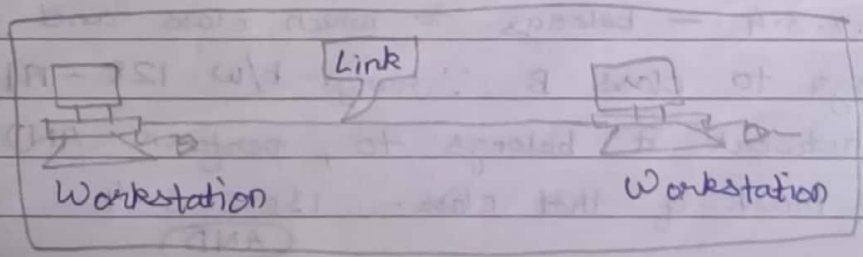
T ≥ 2 * PD
L ≥ 2 * PD
BW

p- persistent CSMA: Used for slotted channels.
When station becomes ready to send, it senses the channel.
If channel is idle, station transmits within that slot with prob. p and defers from sending with a prob. $q = 1-p$.
If $p > p$, then station transmits, else doesn't transmit and again checks if $p > q$ or $q < p$. This process is repeated until either frame has been transmitted or another station has started transmitting

Broadcast Links: Have single communication channel shared by all machines on network. Data to be transmitted is converted in small packets. Each packet contains address field of destination station. When same data packets are sent to all stations, it is called broadcasting. When packets are sent to specific group of stations, it is multicasting.



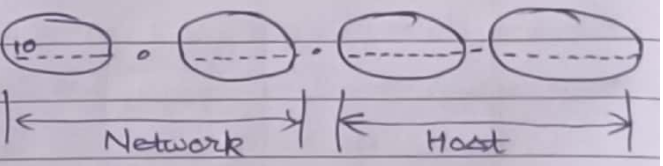
Point to Point Networks
Point - to - point networks provide link b/w any two stations.
Data packets are sent from source station to destination station.
Such a transmission is called unicasting.
Eg. of this transmission is telephone.



* Class A in IP Addressing
→ Has 8 bit network address and 24 bit host address.
→ First bit in network address is dedicated to indicating network class, leaving 7 bits for actual network address.
→ No. of networks in class A = $2^7 - 2 = 128 - 2 = 126$ bcoz. 0.0.0.0 is null address and 127.0.0.0 is used for loopback.
→ No. of hosts possible in every network is $2^{24} - 2$ bcoz the first address in any IP address, is used to represent network and the last address is used to represent broadcast (Network → 64.0.0.0, Broadcast → 64.255.255.255).
→ Millions of class A addresses are wasted as no. of address available in class A is huge.

* Class B in IP Addressing
- Range = 128 - 191
- No. of networks = First 2 bits of two octets are prefix. So remaining 14 bits are there. ∴ 2^{14} = No. of network.

No. of addresses = 2^{30} bcoz



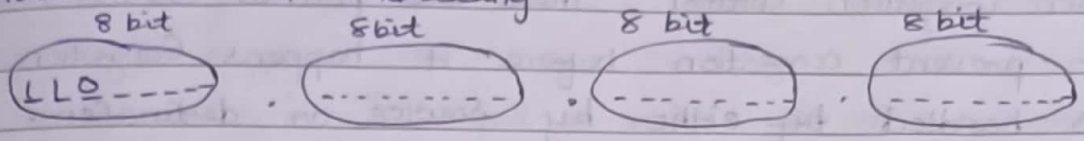
↓

Range is from 128 to 191 that is 64.
And in each bit there are 256 possibilities. So 64 × 256 no. of ~~addr~~ networks i.e $2^6 \times 2^8 = 2^{14}$ networks.
- No. of hosts in each network = 2^{16} but no. of usable hosts = $2^{16} - 2$ bcoz 1st and last are not available for use since 1st is host and last is broadcast.

Eg: 130.2.3.4 — belongs to which class and which network
Ans Belongs to class B ∴ range b/w 128 - 191. To find out the network it belongs to, perform AND operation with default mask of that class.

130.2.3.4
AND
255.255.0.0

* Class C in IP Addressing.



Range = 192 - 223

No. of addresses = 2^{29} since 1st 3 bit of 1st octet are prefixed.

First 3 octets are kept reserved for network. First 3 bits of 1st octet are kept reserved as prefix. ∴ 2^{21} no. of networks in class C. In 1st octet there are 32 IP addresses and for each value there are 8 bits.

No. of hosts in each networks = $2^8 - 2 = 254$.

* Classless Addressing : ① The problems with classful addressing are (i) Millions of addresses were wasted in class A, many were wasted in B and C. (ii) The addresses in class D were too small to meet the need of organisation. (iii) Class D addresses were used for multicast routing and hence they were available as single blocks only. (iv) Class E addresses were reserved.

② To overcome those problems, classless addressing was introduced.

③ To reduce the wastage of IPs, subnetting is used.

④ The process of dividing the IP addresses into smaller sub-blocks is called subnetting.

⑤ The use of subnetting reduces network traffic, optimizes network performance.

⑥ We give IP addres and define number of bits for a mask along with it (usually followed by a '/' symbol) like 192.168.1.1/28

⑦ Here subnet mask is found by putting given number of bits out of 32 as 1, like in given address, we need to put 28 out of 32 bits as 1 and rest as 0. So subnet mask would be 255.255.255.240

Congestion Control Techniques

Open Loop Congestion Control : These are policies which are applied to prevent congestion before it happens. Congestion control is handled by either by source or destination.

Retransmission Policy : • Policy in which retransmission of packets are taken care. If sender feels that sent packet is lost or corrupted then packets needs to be retransmitted.
This transmission may increase congestion in network.
To prevent congestion, retransmission timers must be designed.

Window Policy : • The type of window at sender side may affect Congestion. Several packets in Go-back-n window are resent, although some packets may be successfully received at receiver side.
This duplication may increase congestion in network.
Therefore, selective repeat window should be adopted as it sends specific packets that may have been lost.

Discard Policy : • A good discarding policy adopted by routers is that routers may prevent congestion and at same time partially discard the corrupted or less sensitive packets.

Acknowledgement Policy : • The ack. policy imposed by receiver may also affect congestion.
The receiver should send ack. for N packets rather than for single pack
The receiver should send an ack. only if has to send a pack or a timer expires.

Admission Policy : • Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of congestion in network, router should deny establishing a virtual network connection to prevent further congestion.

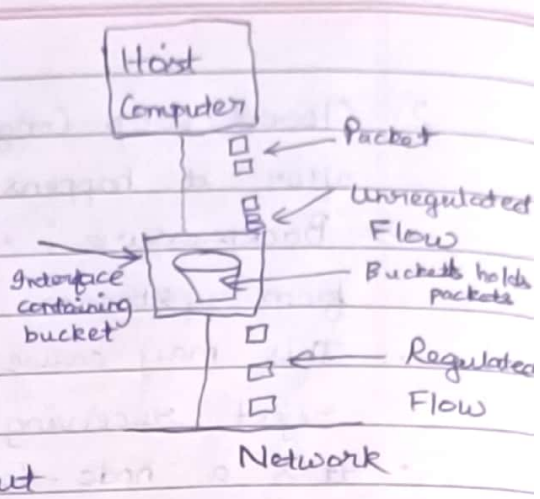
2. Closed Loop Congestion Control: Technique used to treat congestion after it happens.

→ Backpressure: • Technique in which congested node stops receiving packets from upstream node.
• This may cause upstream nodes to become congested and reject receiving data from above nodes.
• It's a node-to-node congestion control technique that propagate in opposite direction of data flow.
• Can be applied only to virtual circuit where each node has info of its above upstream nodes.

→ Choke packet technique: • Applicable to both virtual network and datagram subnets.
• It's a packet sent by node to source to inform it of congestion.
• Each router monitors its resources and utilization at each of its output lines.
• Whenever the resource utilization value exceeds threshold, set by admin, the router directly sends a choke packet to source giving feedback to reduce traffic.
• The intermediate nodes through which packets have travelled aren't informed about congestion.

→ Implicit Signaling: • No communication b/w congested nodes and source.
• The source guesses that there's a congestion in network.
• Eg: when sender sends several packets but there's no ack. for a while, the source guesses that there is congestion.

→ Explicit Signaling: • If node experiences congestion, it directly informs source or destination about congestion through a packet.
• Diff b/w explicit signaling & choke packet is that signal is included in packets that carry data rather than creating diff packet.
• Explicit signaling can occur in forward/backward direction.

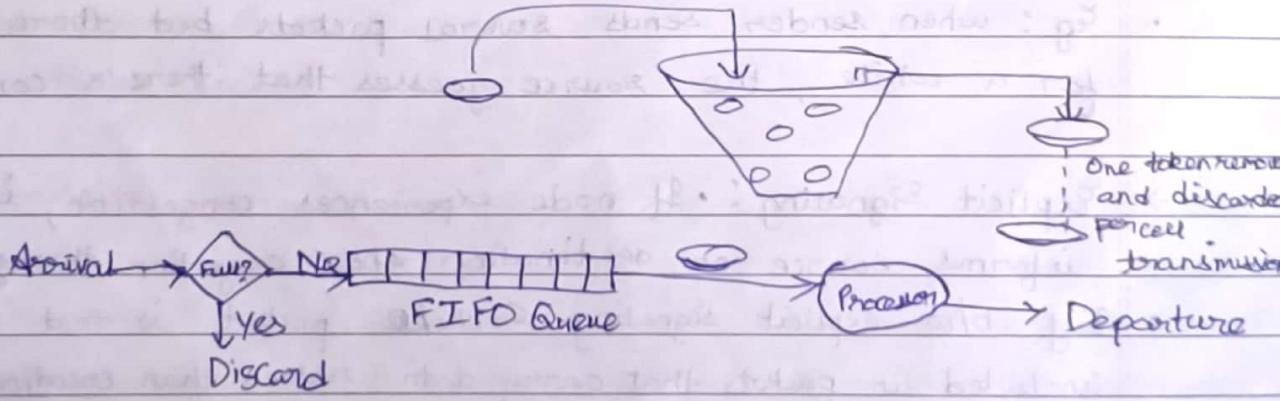


* Leaky Bucket Algo:

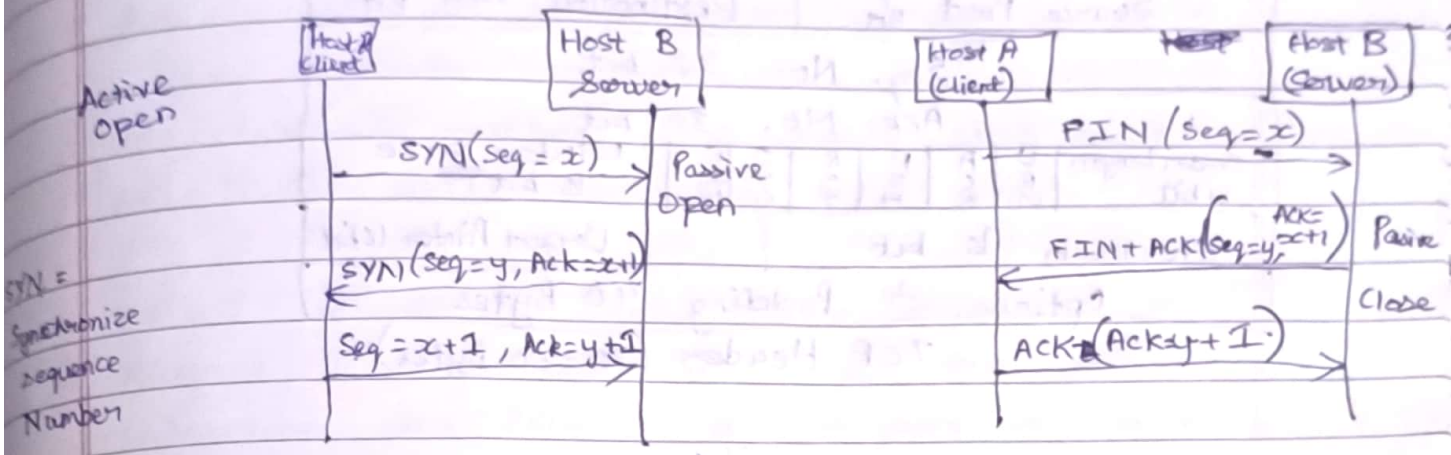
- Traffic shaping mechanism which shapes bursty traffic into fixed rate by averaging the data rate.
- Imagine the case where water is poured in a bucket with hole.
- The input speed of water is variable but water comes out of hole at a constant rate.
- Same concept can be applied to packets in network.
- Data comes from source at variable speeds but while going out of the bucket, it goes out with constant speed.
- One disadvantage is if the bucket is full, then data coming in will not be included in bucket and data will be lost.

* Token Bucket Algo:

- Leaky bucket algo allows only avg. flow rate of data.
- Can't deal with bursty data and doesn't consider idle time of host.
- Token bucket allows bursty data transfers. Tokens generated at every clock tick.
- For packets to be transmitted, system must remove tokens from packets.
- Thus, token bucket allows idle hosts to accumulate credit for future in form of tokens.



TCP Handshake – Used in Client Server communication. Whenever reliability is needed. Works in full duplex mode i.e. client sends data to server & vice versa is also possible.



Three steps in 3 way handshaking: ① Connection established - Done when OS assigns a specific PORT to clients and it requests the server to establish a connection with it by sending a connection request which consists of a SYN, TCP Header, and Acknowledgement.

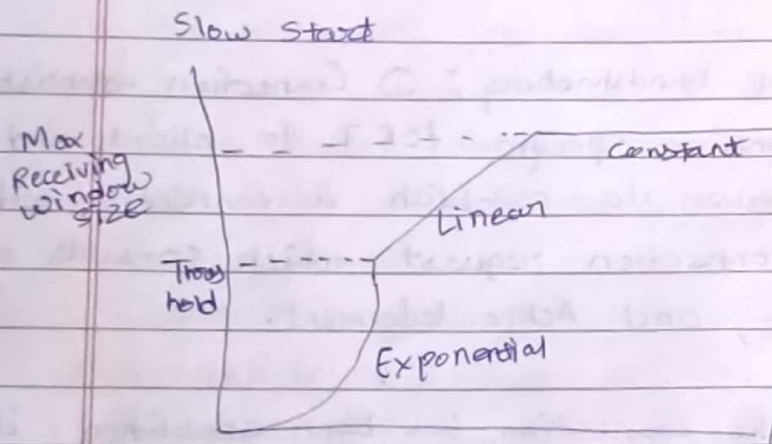
② Data transfer: After the connection has been established, it is time for client and server to transfer data. Before this, both clients and server establish their buffers and reserve them for the time when data arrives. When data and its ack. are sent together, then it is called piggyback package. Piggback is used to reduce traffic in network.

③ Client Termination: 4 step process. Client sends FIN packet to server. The FIN packet may contain data along with it. When FIN packet is received by server, it frees up the resources. Then the connection becomes half duplex and now only server can send data. After this, server will also send an ack and fin packet to totally terminate the connection.

TCP Header: Header is sent along with data. It adds various functionalities. From App. layer, data is coming continuously to Trans. Layer. Then TCP converts this continuous flow of data to segment of bytes.

Source Port 16 Bit	Destination Port 16 Bit
Seq. No. 32 bit	
Ack. No. 32 bit	
Header Length 4 bit | URG | ACK | PSH | RST | SYN | FIN	Window Size 16 bit
Checksum 16 bit	Urgent Pointer 16 bit
Options & Padding 40 Bytes	

TCP Header (20-60 Bytes).



2 Cases:
- Timeout occured: Severe Congestion
- 3 Ack Received: Light Congestion

- TCP slow start is an algo. which balances the speed of a network connection.
- TCP slow start is one of the first steps in congestion control process.
- A sender attempts to communicate to a receiver. The sender's initial packet contains a small congestion window, which is determined based on the sender's max. window.
- The receiver acknowledges the packet and responds with its own window size. If the receiver fails to respond,

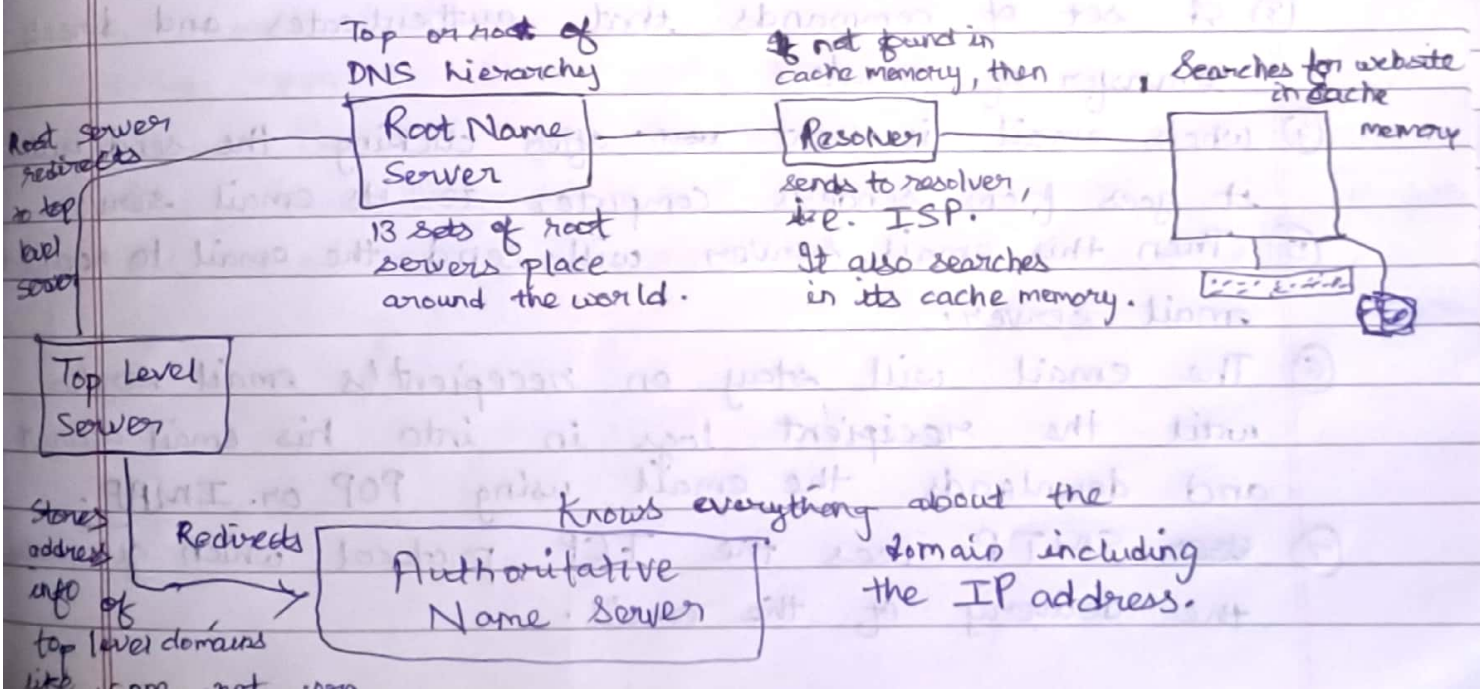
→ When congestion occured, than start from beginning.

→ When congestion occured than start from threshold value.

the sender knows not to continue sending data.

- After receiving the acknowledgement, sender increases the next packet's window size. The window size gradually increases until the receiver can no longer acknowledge each packet, or until either ~~window~~ sender or receiver's window limit is reached.
- Once limit is reached, the job of slow start is done and other congestion control algos take over.

* DNS : ① Stands for Domain Name System.
② Humans generally deal with names but computers only understand the language of .0s and 1s. To bridge this gap b/w humans and computers, DNS was designed.
③ It resolves domain names to IP addresses.
④ A website can be accessed by either its Domain Name or its IP address.
⑤ Domain Name and IP address are unique for each website.
⑥ There are various types of domain : .com, .org, .gov, .edu, etc.



HTTP : ① Stands for Hypertext Transfer Protocol.
② Used for viewing web pages.
③ In HTTP, all the information is sent in plain text format.
④ This makes it easier for attackers to intercept the message.
To overcome this, HTTPS was designed.
HTTPS is same as HTTP but it adds a layer of security by encrypting the plain text sent over internet.
Uses encryption algos. to scramble the data being transferred.
HTTPS uses SSL (secured socket layer) protocol for protection of data.
SSL uses public key encryption to secure data.
② When computers connect to a website, the computers ask the website to identify itself. Then the websites provide an SSL certificate which is used to authenticate identity of a website.

SMTP : ①. Stands for Simple Mail Transfer Protocol.
② Used for sending emails over the internet.
③ A set of commands that authenticates and directs the transfer of emails.
When email is sent after clicking the send button, it goes from sender's computer to its email server.
④ Then this email server will send the email to recepient's email server.
The email will stay on recepient's email server, until the recipient logs in into his email account and downloads the email using POP or IMAP.
SMTP uses the TCP protocol which guarantees the delivery of the email.

* FTP: ① Stands for file transfer protocol.
② used for transferring files over a network.
③ FTP is the language that computers use to transfer files over a TCP/IP network.
④ A sender can upload the files on a FTP server and user can download that file from that FTP server.
⑤ FTP servers may require users to create an account with email and password.
⑥ A drawback of FTP is that it isn't a secure protocol.
⑦ Data being transferred is in the plain text format.
⑧ FTP uses port number 21 for control connection.
⑨ FTP uses port number 20 for data connection.

* Telnet: ① Stands for teletype network.
② It is a client-server app. that allows a user to log onto remote machine and lets user to access any app on remote computer.
③ Telnet uses NVT (Network Virtual Terminal) system to encode characters on local system.
④ On server machine, NVT decodes characters to a form acceptable to remote machine.
⑤ Many apps are built using telnet.
⑥ Uses Port 23 for its services.
⑦ Only uses commands and no use of GUI makes it fast.
⑧ All data sent in plain text form, hence unsafe.

* Routing Algorithms :

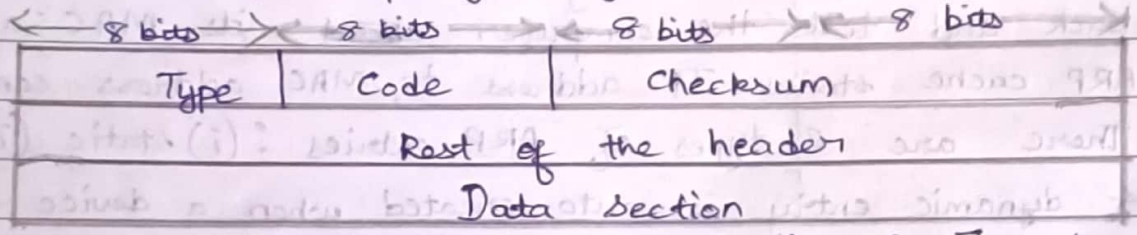
- Link State Routing : ① Technique in which each router shares the knowledge of its neighbourhood with every router in the network. This is called flooding.
② Here instead of sending the entire routing table, as in case of distance vector routing, only the distance routes are sent.
③ Link state routing has 2 phases : (i) Reliable Flooding
Initial State : Each node knows the cost of its neighbour.
Final State : Each node knows the entire graph.
(ii) Route Classification : Since flooding is used in link state routing, the problem of high bandwidth and high congestion arise.

- Distance Vector Routing : ① Each router maintains a routing table separately, giving the best known distance (shortest) to each destination and which link to use to get there.
② Only distance vector is shared and that too with neighbours only.
③ Uses the bellman - ford algo. to calculate shortest path.
④ Convergence time can be slow.
⑤ If there is a change in network topology, it may take some time for routers to converge to new best paths. This is count - to - infinity problem.
⑥ RIP (Routing Internet Protocol) is a common distance vector routing protocol used in small to medium-sized networks.

- ARP : ① Stands for Address Resolution Protocol.
② Used to resolve IP addresses to MAC addresses.
③ The main task of ARP is to convert 32-bit IP address to a 48-bit MAC address.
④ Used when one device wants to communicate with another device on a local network.
⑤ All operating systems, ~~that~~ in an IPv4 network keep an ARP cache.
⑥ In order to find MAC address, computer will first look for it in its ARP cache.
⑦ If not found then it will broadcast the message on the network asking every computer ~~that~~ if it has the specific IP address and will ask for the MAC address.
⑧ Then the computer having the IP address will respond back and tell the computer ~~[redacted]~~ its MAC address.
⑨ ARP cache stores IP address to MAC address connections.
⑩ There are 2 types of ARP entries : (i) static (ii) Dynamic.
⑪ A dynamic entry is auto created when a device sends out a broadcast request for MAC address.
⑫ Static entry is when someone manually enters the IP address to MAC address association.

- RARP : ① Stands for reverse address resolution protocol.
② Protocol by which a physical machine in a LAN can request to learn IP address from an ARP table/cache.
③ A network administrator creates a table in LAN gateway router that MAPS MAC address to IP address.
④ RARP is available for Ethernet, token ring LANs.

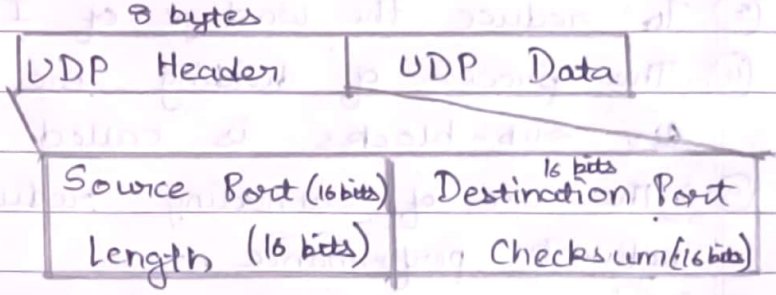
- ICMP : ① Stands for Internet Control Message Protocol.
② It is a network layer protocol.
③ It is used for error handling in network layer.
④ Primarily used on network devices such as routers.
⑤ If a sender wants to send message to some destination, but router couldn't send the message, then router informs the sender that it couldn't send the message.
⑥ The IP protocol does not have any error-correcting mechanism, so it uses a message to convey the info.
⑦ ICMP messages are divided into two categories :
(i) error-reporting : when routers encounter a problem while processing an IP packet.
(ii) Query messages : Query messages are those that help the host to get specific info about other host. Eg- client, ser



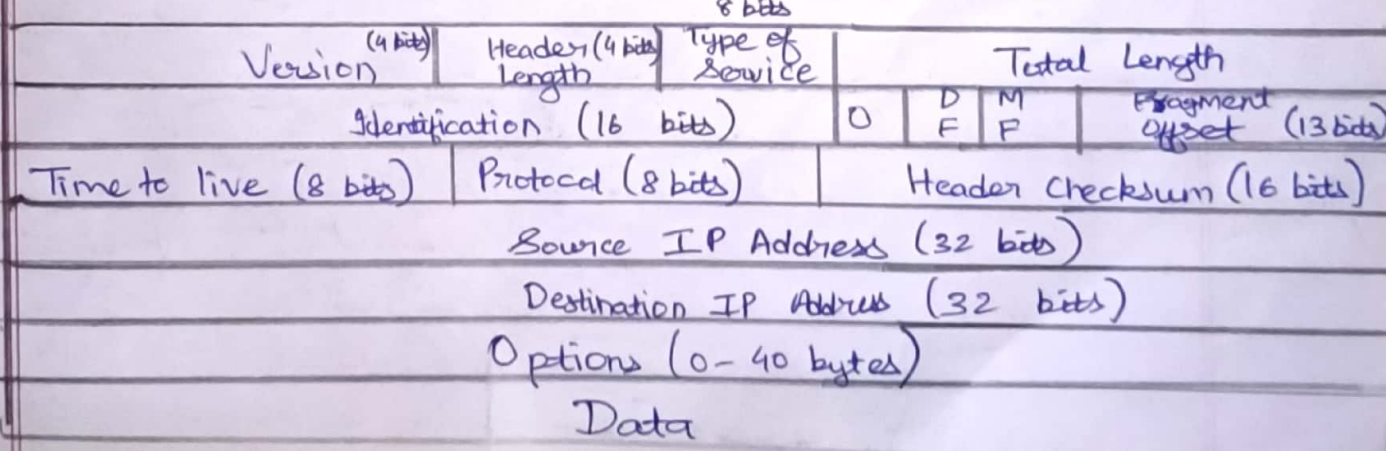
ICMP Message Format

- IGMP : ① Stands for Internet Group Management Protocol.
② Allows several devices to shares one IP address so they can all receive ~~dest~~ the same data.
③ It is a network layer protocol used to set up multicasting on networks that use IPv4.
④ IGMP uses IP addresses that are set aside for multicasting. The addresses range b/w 224.0.0.0 to 239.255.255.255.
⑤ Each multicast group share one of those IP addresses.
⑥ Any device can leave or join a group at any time.

* UDP : ① Stands for User Datagram Protocol.
② It is a connectionless protocol.
③ UDP is reliable as it does not guarantee the delivery of message.
④ UDP is fast because it is connectionless and also because it doesn't have mechanisms for error correction.
⑤ High performance is needed, UDP permits packets to be dropped instead of processing delayed packets.
⑥ UDP is efficient both in terms of latency and bandwidth.



* IPv4 Protocol : ① Stands for Internet Protocol Version 4.
② It is a protocol that uses datagram to communicate over internet.
③ The IP protocol operates at network layer protocol of OSI model.
④ In IPv4, each endpoint is identified by one or more globally unique IP address.
⑤ An IP network normally uses a dynamic routing protocol to find alternate routers whenever a link becomes unavailable.



* Bluetooth :

- It is a wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances.
- This technology was invented by Ericson in 1994.
- It operates in unlicensed, industrial, scientific and medical (ISM) band at 2.69 GHz to 2.485 GHz.
- Bluetooth lets devices discover and connect to each other by pairing, and then securely transfers data.
- Ranges upto 10 metres and max. devices connected simultaneously can be 7.
- A bluetooth network is called Piconets and a collection of interconnected Piconets is called Scatternet.

* Piconet :

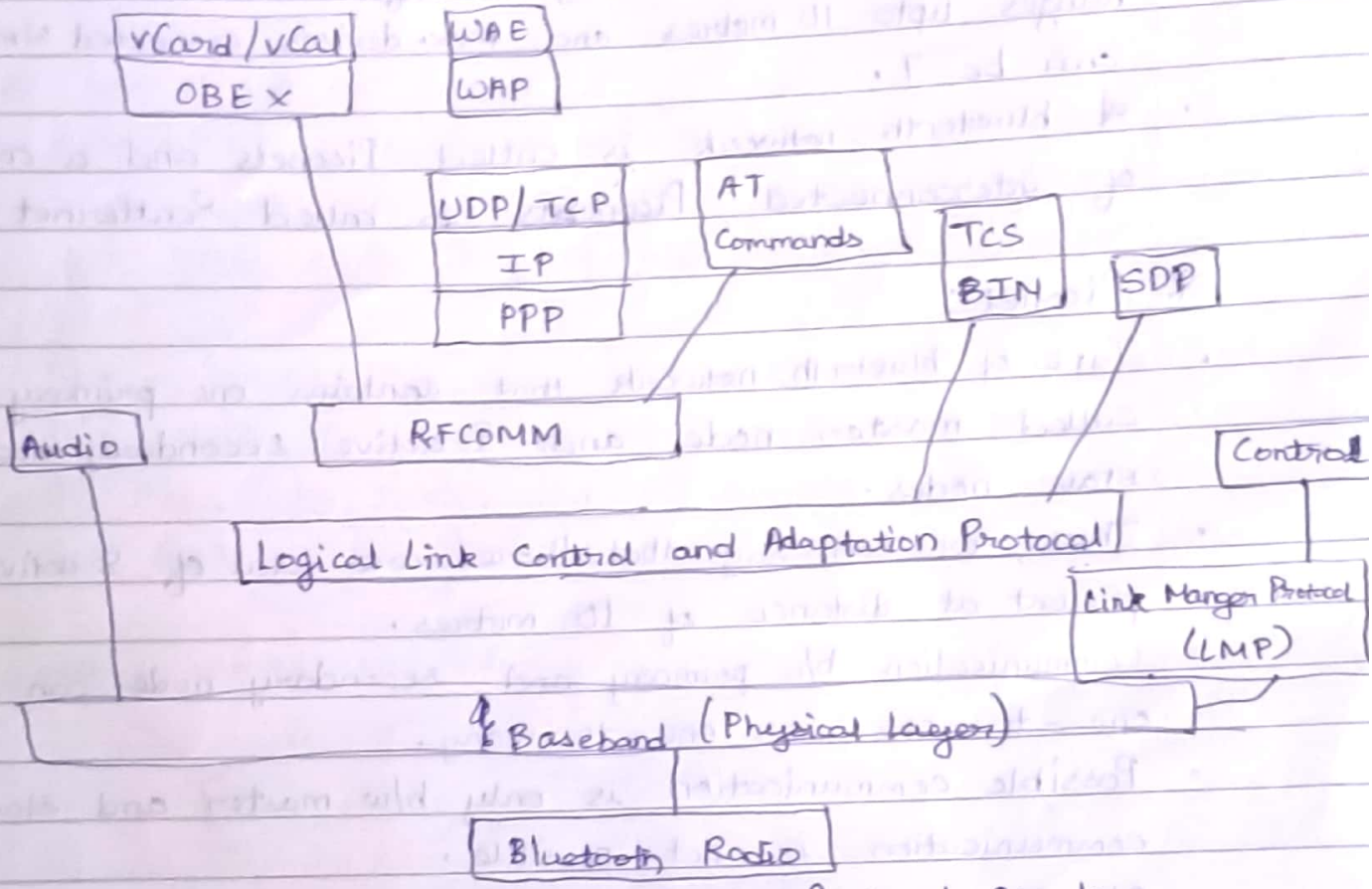
- Type of bluetooth network that contains one primary node called master node, and 7 active secondary nodes called slave nodes.
- Thus, we can say that there are total of 8 active nodes present at distance of 10 metres.
- Communication b/w primary and secondary node can be one-to-one or one-to-many.
- Possible communication is only b/w master and slave, slave-slave communication is not possible.
- It also has 255 parked nodes, these are secondary nodes and cannot participate in communication unless it gets converted to active state.

* Scatternet :

- It is formed by using various piconets.
- A slave that is present in one piconet can act as master or we can say primary is other piconet.

- This kind of node can receive message from master in one piconet and deliver the message to its slave into other piconet where it is acting as a slave.
- This type of node is called bridge node.
- A station cannot be master in two piconets.

* Bluetooth Protocol Stack



- Heart of bluetooth specification is Protocol Stack.
- By providing well-defined layers of functionality, bluetooth specification ensures interoperability and encourage the adoption of bluetooth technology.

⇒ Radio : Defines physical layer specs for radio wave transmi including air interface, frequency band, modulation.

⇒ Basebands : Addresses packet frame, timing and power control

⇒ Link Manager protocol : Establishes logical link b/w bluetooth devices, managing authentication, encryption, packet size negotiati

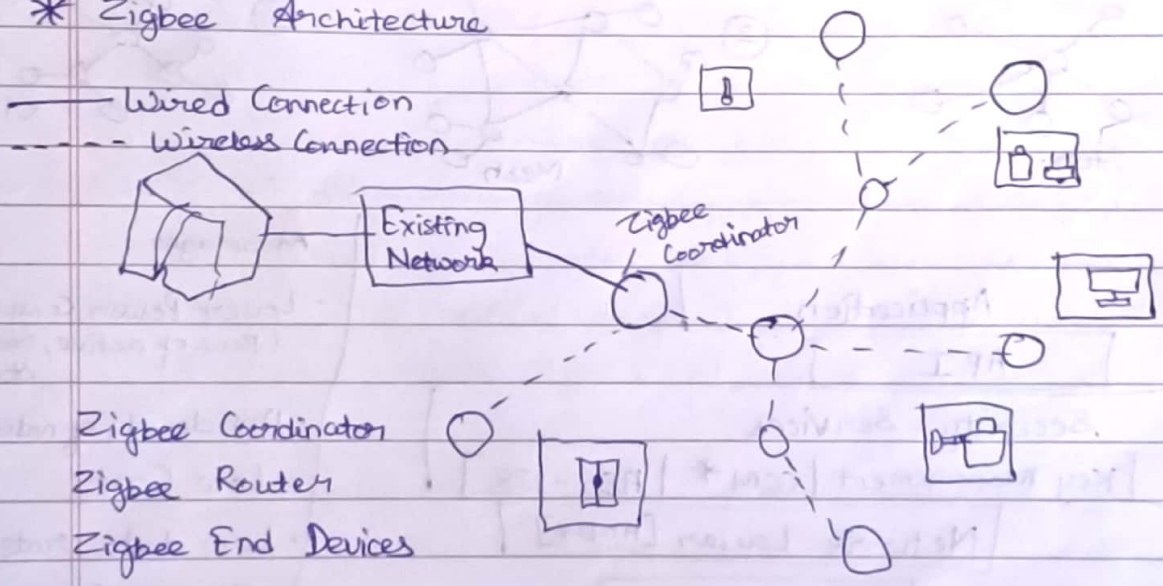
⇒ Logical link Control & and Adaptation Protocol (L2CAP) : Adapts frame formats b/w upper and baseband layers, supporting both connection orientation and connectionless services.

⇒ Service Discovery Protocol (SDP) : Handles service queries fo device info, facilitating connection b/w bluetooth devices.

ZIGBEE

- Built for control and sensor networks on IEEE 802.15.4 for WPAN.
- Operates on 2.4 GHz frequencies.
- Data rate is 250 Kbps.
- Two way transmission of data b/w sensors and controller
- Range is 10 - 100 metres.

* Zigbee Architecture



⇒ Zigbee Coordinator: Responsible for storing and handling info. Receiving and transmitting operations are done using coordinator.

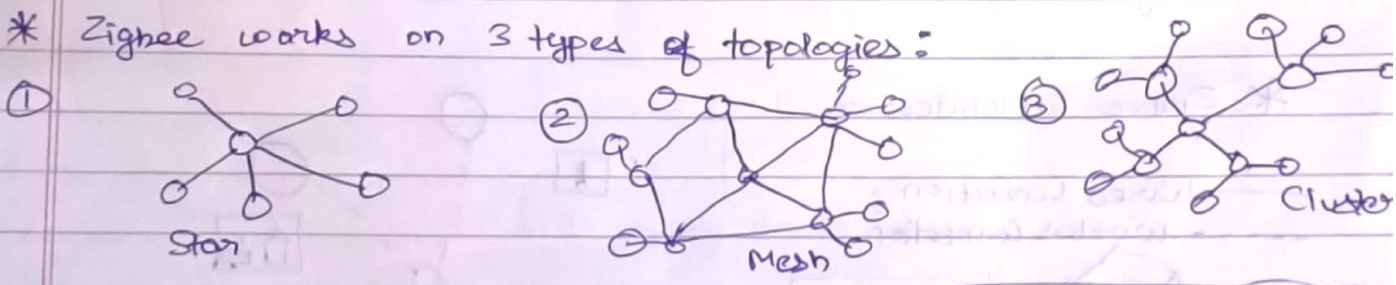
⇒ Zigbee Router: Permits data to pass to other devices.

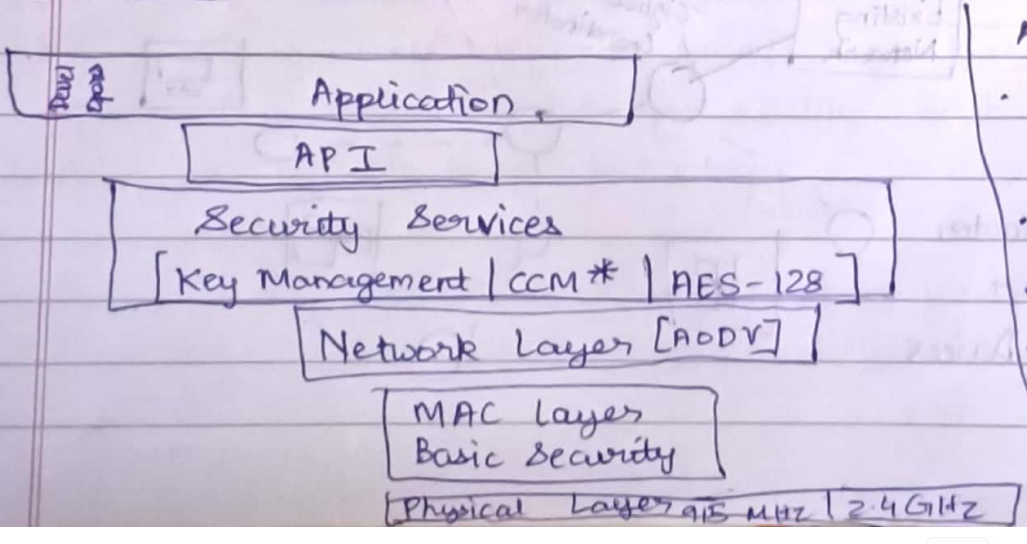
⇒ Zigbee End Devices: End devices have limited functionality to communicate with parent nodes

* Two modes of Zigbee

- Beacon: where there is no data communication from end devices, the router and coordinator enters sleep state. This mode work for time slots. They operate when communication is needed.
- Non - Beacon: The coordinator and router continuously monitor this state of incoming data, hence more power is consumed In this mode, router and coordinator don't sleep bcoz at any time any node can wake up and communicate.

* Zigbee works on 3 types of topologies:





Advantages

- Lower Power Consumptio (Bcoz of active, Sleep modes)
- High density of nodes/ne
- Low Cost
- Low data rate
- Simple implementat